A Panel to Discuss Future Security in the AG

Deb Agarwal – Moderator

(includes material borrowed from Bob Olson and Mary Thompson)

Assumptions

- Need secure systems for meetings
- Want security hat works and is easy to use
- Want to allow only a particular set of users and nodes into a meeting
  - Identify attending users and nodes
  - Specify allowed users
  - Enforce security
- Denial of service for legitimate users has serious consequences and leads to use of insecure systems if available or lack of adoption

Panel

- Deb Agarwal - moderator
- Bob Olson – AG developer
- Abdelilah Essiari – security capabilities developer
- Chris Willing – AG user

Agenda

- 15 minute presentations by each panelist
- 30 minutes for discussion

X.509 Certificates

- Public key infrastructure
  - Two part unique pair (public/private)
  - Private key stored locally encrypted with pass phrase
  - Sign a document using private key – verify using public
  - Encrypt using public key – decrypt using private
- Certificate authority
  - Issues certificates (typically identifies bearer)
  - Signs certificates
- A certificate typically contains the:
  - Owner's name (unique for the CA)
  - Expiration date
  - Name of the issuing CA
  - Owner's public key
  - Signature of the issuer
- Standardized format for certificates

Five elements of Authentication

- Person, principal or entity
  —What is being authenticated?
- Distinguishing characteristic
  —What does the entity hold that allows proof?
- Proprietor
  —What party is requiring the authentication?
- Authentication mechanism
  —How is the proof of identity actually achieved?
- Access control mechanism
  —How is the authenticated identity used?

Validation

- During authentication, each party validates the identity provided to it
- Validation can be considered a series of questions
- A “no” answer to any of the questions results in failure of validation…
- Which results in the failure of the attempted communication.

Validation 1.

- Was the certificate presented issued by a Certificate Authority that I trust?
  - —The process presented with a certificate must hold the identity cert for the CA which issued the cert in question
  - —Digital signature of the presented cert verified with the public key in the CA cert
  - —CA cert must be available, and signature verified, for validation to succeed.

Validation 2.

- Is the certificate currently valid?
  - —Each certificate has a well-defined range of time when it is considered valid.
  - —For validation to succeed, the current time must fall within that range.
  - —Each issuing CA certificate must also be within its time of validity.

Validation 3.

- Does the entity presenting the cert hold the private key corresponding to the cert?
  - —A process requesting authentication must provide proof it holds the private key
  - —Proof typically takes the form of the requesting process encrypting a random challenge with the private key

Certification Chains

- A Certificate Authority can delegate the authority to sign certificates to a subordinate CA
- Each subordinate CA also has an identity certificate
- Validation of an identity issued by a sub-CA requires checking of all certificates in the chain.

Mutual Authentication

- Defined as authentication process where both client and server both present certificates
- Each party authenticates the other's identity
- AG Toolkit based on mutual authentication via Globus Toolkit

Authorization

- Based on authentication
- Determine whether entity is authorized to do what it is requesting to do
- Either determined locally or by an authorization server
  - — Access control lists
  - — Policy stored at a server
- Provides an answer of yes or no typically

Enforcement

- Put the answer from the authorization into action
- Restricts access to particular actions authorized
- Relies on the software providing the action to consider authorization

Additional Security Definitions

Privacy

- Typically use encryption
- Shared symmetric session key

Proxy

- Public/private key pair
- Generated by and signed by the entity
- Stored unencrypted
- Allows authentication without providing pass phrase

Questions

- What is the right model for handling authorization of people in the venues versus authorization of the venues?
- Are there sites that have restrictions not being served by the AG model? (e.g. due to site requirements for kerberos)
- Do we need spaces in the AG that do not require authentication and authorization? (e.g. lobby and test room)
- Time to authenticate I Access
- Control over authorization for individual Venues
- Easy setup of a secure meeting
- Firewalls
- User can easily understand how to do what they want